PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-197054
(43)Date of publication of application : 19.07.2001

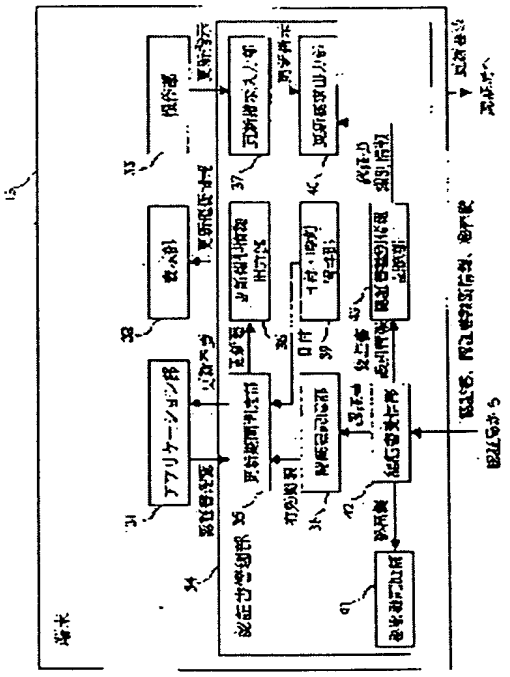
(51)Int.Cl. H04L 9/32
G06F 13/00
G06F 17/60
G09C 1/00

(21)Application number : 2000-000893
(22)Date of filing : 06.01.2000

(71)Applicant : MITSUBISHI ELECTRIC SYSTEMWARE CORP
(72)Inventor : NISHINA KOICHI
NAGASAKA ATSUSHI

(54) DEVICE AND METHOD FOR WRITTEN AUTHENTICATION MANAGEMENT AND COMPUTER-READABLE RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the validity of a written authentication from expiring, to provide pleasant operability for a user, and to accelerate the smooth operation of a system as to a written authentication management device which manages written authentication.
SOLUTION: An update period decision part 35 decides whether update is needed based on the term of validity included in a written authentication stored in a written authentication storage part 38 and the date managed by a date and time management part 39 and when it is decided that the update is needed, an update urging information output part 36 outputs information urging the update.



LEGAL STATUS

[Date of request for examination] 21.09.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－197054
（P2001－197054A）
(43)公開日　平成13年７月19日(2001.7.19)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	13/00	３５４Ｚ	５Ｂ０４９
Ｇ０６Ｆ	13/00	３５４	Ｇ０９Ｃ	1/00	６４０Ｚ	５Ｂ０８９
	17/60		Ｈ０４Ｌ	9/00	６７５Ｄ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０	Ｇ０６Ｆ	15/21	Ｚ	
			Ｈ０４Ｌ	9/00	６７５Ｂ	

審査請求　未請求　請求項の数22　ＯＬ　（全 13 頁）

(21)出願番号　特願2000－893(P2000－893)

(22)出願日　平成12年１月６日(2000.1.6)

(71)出願人　394013002
三菱電機システムウェア株式会社
神奈川県横浜市戸塚区川上町87番地１

(72)発明者　仁科　浩一
神奈川県横浜市戸塚区川上町87番地１　三菱電機システムウェア株式会社内

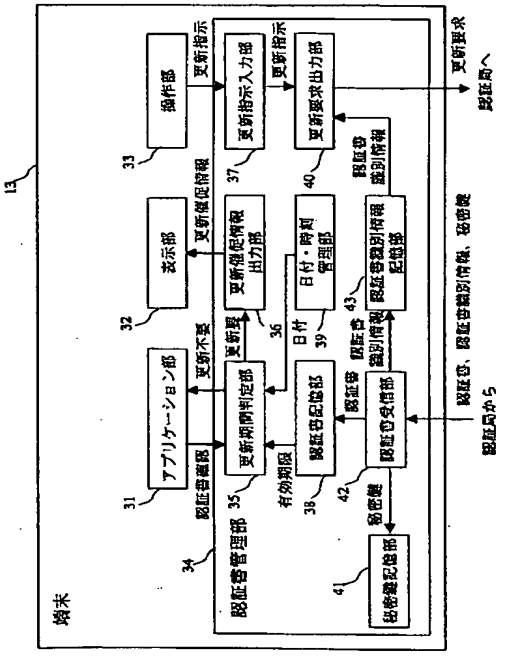
(72)発明者　長坂　敦
神奈川県横浜市戸塚区川上町87番地１　三菱電機システムウェア株式会社内

(74)代理人　100099461
弁理士　溝井　章司

最終頁に続く

(54)【発明の名称】　認証書管理装置及び認証書管理方法及びコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　認証書を管理する認証書管理装置に係り、認証書の有効期限切れを未然に防止し、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼動を促進することを課題とする。
【解決手段】　更新期間判定部３５は、認証書記憶部３８が記憶する認証書に含まれる有効期限と、日付・時刻管理部３９が管理する日付とに基づいて更新期間であるか否かを判定し、更新期間であると判定した場合には、更新催促情報出力部３６が、更新を催促する情報を出力する。



1

【特許請求の範囲】

【請求項１】　以下の要素を備えることを特徴とする認証書管理装置

（１）有効期限を含む認証書を記憶する認証書記憶部

（２）日付を管理する日付管理部

（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する更新期間判定部

（４）上記更新期間判定部によって、更新期間であると判定した場合に、更新を催促する情報を出力する更新催促情報出力部。

【請求項２】　上記更新期間判定部は、上記日付から上記有効期限までの期間が所定の日数に満たない場合に更新期間であると判定することを特徴とする請求項１記載の認証書管理装置。

【請求項３】　上記認証書管理装置は、認証局と他の認証書管理装置と接続し、

上記認証書管理装置は、更に、更新要求を認証局に出力する更新要求出力部と、

更新された認証書を受信する認証書受信部と、

受信した認証書を他の認証書管理装置へ送信する要否を確認する情報を出力する認証書送信要否確認情報出力部と、

認証書送信指示を入力する認証書送信指示入力部と、

認証書送信指示が入力された場合に、受信した認証書を他の認証書管理装置へ送信する認証書送信部とを有することを特徴する請求項１記載の認証書管理装置。

【請求項４】　認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする認証書管理装置

（１）有効期限を含む認証書を記憶する認証書記憶部

（２）日付を管理する日付管理部

（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する更新期間判定部

（４）上記更新期間判定部によって、更新期間であると判定した場合に、更新要求を認証局に出力する更新要求出力部。

【請求項５】　上記更新期間判定部は、上記日付から上記有効期限までの期間が所定の日数に満たない場合に更新期間であると判定することを特徴とする請求項４記載の認証書管理装置。

【請求項６】　上記認証書管理装置は、他の認証書管理装置に接続し、

上記認証書管理装置は、更に、更新された認証書を受信する認証書受信部と、

更新された認証書が受信された場合に、受信した認証書を他の認証書管理装置に送信する認証書送信部とを備えることを特徴とする請求項４記載の認証書管理装置。

【請求項７】　認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする認証書管理装置

2

（１）更新予定日を含む失効リストを記憶する失効リスト記憶部

（２）日付を管理する日付管理部

（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する更新期間判定部

（４）上記更新期間判定部によって、更新期間であると判定した場合に、更新要求を認証局に出力する更新要求出力部。

【請求項８】　上記更新期間判定部は、上記日付が上記更新予定日を過ぎている場合に更新期間であると判定することを特徴とする請求項７記載の認証書管理装置。

【請求項９】　上記更新期間判定部は、上記日付が上記更新予定日と同日である場合に更新期間であると判定することを特徴とする請求項７記載の認証書管理装置。

【請求項１０】　上記認証書管理装置は、更に、認証局から失効リストを受信する失効リスト受信部を有することを特徴とする請求項７記載の認証書管理装置。

【請求項１１】　認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする認証書管理装置

（１）更新予定日を含む失効リストを記憶する失効リスト記憶部

（２）日付を管理する日付管理部

（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する更新期間判定部

（４）上記更新期間判定部によって、更新期間であると判定した場合に、更新を催促する情報を出力する更新催促情報出力部。

【請求項１２】　上記更新期間判定部は、上記日付が上記更新予定日を過ぎている場合に更新期間であると判定することを特徴とする請求項１１記載の認証書管理装置。

【請求項１３】　上記更新期間判定部は、上記日付が上記更新予定日と同日である場合に更新期間であると判定することを特徴とする請求項１１記載の認証書管理装置。

【請求項１４】　上記認証書管理装置は、更に、認証局から失効リストを受信する失効リスト受信部を有することを特徴とする請求項１１記載の認証書管理装置。

【請求項１５】　以下の要素を備えることを特徴とする認証書管理方法

（１）有効期限を含む認証書を記憶する工程

（２）日付を管理する工程

（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する工程

（４）更新期間であると判定した場合に、更新を催促する情報を出力する工程。

【請求項１６】　認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする認証書管理方法

（１）有効期限を含む認証書を記憶する工程
（２）日付を管理する工程
（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する工程
（４）更新期間であると判定した場合に、更新要求を認証局に出力する工程。
【請求項１７】　認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする認証書管理方法
（１）更新予定日を含む失効リストを記憶する工程
（２）日付を管理する工程
（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する工程
（４）更新期間であると判定した場合に、更新要求を認証局に出力する工程。
【請求項１８】　認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする認証書管理方法
（１）更新予定日を含む失効リストを記憶する工程
（２）日付を管理する工程
（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する工程
（４）更新期間であると判定した場合に、更新を催促する情報を出力する工程。
【請求項１９】　以下の処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体
（１）有効期限を含む認証書を記憶する処理
（２）日付を管理する処理
（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する処理
（４）更新期間であると判定した場合に、更新を催促する情報を出力する処理。
【請求項２０】　以下の処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体
（１）有効期限を含む認証書を記憶する処理
（２）日付を管理する処理
（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する処理
（４）更新期間であると判定した場合に、更新要求を認証局に出力する処理。
【請求項２１】　以下の処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体
（１）更新予定日を含む失効リストを記憶する処理
（２）日付を管理する処理
（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する処理
（４）更新期間であると判定した場合に、更新要求を認証局に出力する処理。
【請求項２２】　以下の処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体
（１）更新予定日を含む失効リストを記憶する処理
（２）日付を管理する処理
（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する処理
（４）更新期間であると判定した場合に、更新を催促する情報を出力する処理。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、認証書を管理する認証書管理装置に係り、認証書の有効期限切れを未然に防止し、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼動を促進する認証書管理装置に関する。
【０００２】
【従来の技術】近年、インターネットを介したデータ転送を伴うシステムにおいて、セキュリティの確保の為に、認証局が発行する認証書を用いる方式が一般化している。この認証書には、有効期限が設定されていて、その有効期限を過ぎてしまった場合には、認証局に対して、改めて新しい認証書の発行を要求しなければならず、その手間は煩わしく、システムの円滑な稼動を阻害する。
【０００３】また、有効期限内に認証書を更新することによって、継続的にシステムを稼動させることもできるが、認証書の更新の為のオペレーションは、一般のユーザーにとって煩わしいものである。認証書の更新の必要性は、ユーザーに提供するシステムの機能と直接的に関係が無い場合が多い。そのような場合に、ユーザーは、このオペレーションをセキュリティの確保の為に必要な行為であると納得することは出来ず、単に煩雑な印象を与えるものとなる。
【０００４】一方、認証書が何らかの理由により、有効でなくなる場合がある。認証局は、このような失効した認証書を一元的に管理し、失効した認証書のリストである失効リストを作成している。システムを構成する端末は、認証局に失効リストを要求し、受信した失効リストに基づいて、失効した認証書の使用を禁止し、認証書の有効性を担保している。しかし、各端末側では、この失効リストを常に最新のものに更新しておかなければならず、更新の為の管理行為は、ユーザーに対して過大な負担を与えている。また、ユーザーが更新を怠った場合には、認証の有効性が保たれないおそれが生じる。
【０００５】
【発明が解決しようとする課題】本発明は、上記した従来技術の欠点を除くためになされたものであって、その目的とするところは、認証書の有効期限を過ぎる前に、

ユーザーに認証書の更新を促し、認証書の有効期限切れを未然に防止することである。

【０００６】また、認証書の更新手続き自体を、自動化し、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼動を促進する。

【０００７】更に、失効リストの更新を自動化し、ユーザーの管理行為の負担を軽減し、併せて失効リストが最新であることを保証し、認証の有効性を担保する。

【０００８】

【課題を解決するための手段】本発明に係る認証書管理装置は、以下の要素を備えることを特徴とする。

（１）有効期限を含む認証書を記憶する認証書記憶部

（２）日付を管理する日付管理部

（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する更新期間判定部

（４）上記更新期間判定部によって、更新期間であると判定した場合に、更新を催促する情報を出力する更新催促情報出力部。

【０００９】更に、上記更新期間判定部は、上記日付から上記有効期限までの期間が所定の日数に満たない場合に更新期間であると判定することを特徴とする。

【００１０】更に、上記認証書管理装置は、認証局と他の認証書管理装置と接続し、上記認証書管理装置は、更に、更新要求を認証局に出力する更新要求出力部と、更新された認証書を受信する認証書受信部と、受信した認証書を他の認証書管理装置へ送信する要否を確認する情報を出力する認証書送信要否確認情報出力部と、認証書送信指示を入力する認証書送信指示入力部と、認証書送信指示が入力された場合に、受信した認証書を他の認証書管理装置へ送信する認証書送信部とを有することを特徴する。

【００１１】本発明に係る認証書管理装置は、認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする。

（１）有効期限を含む認証書を記憶する認証書記憶部

（２）日付を管理する日付管理部

（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する更新期間判定部

（４）上記更新期間判定部によって、更新期間であると判定した場合に、更新要求を認証局に出力する更新要求出力部。

【００１２】更に、上記更新期間判定部は、上記日付から上記有効期限までの期間が所定の日数に満たない場合に更新期間であると判定することを特徴とする。

【００１３】更に、上記認証書管理装置は、他の認証書管理装置に接続し、上記認証書管理装置は、更に、更新された認証書を受信する認証書受信部と、更新された認証書が受信された場合に、受信した認証書を他の認証書管理装置に送信する認証書送信部とを備えることを特徴とする。

【００１４】本発明に係る認証書管理装置は、認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする。

（１）更新予定日を含む失効リストを記憶する失効リスト記憶部

（２）日付を管理する日付管理部

（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する更新期間判定部

（４）上記更新期間判定部によって、更新期間であると判定した場合に、更新要求を認証局に出力する更新要求出力部。

【００１５】更に、上記更新期間判定部は、上記日付が上記更新予定日を過ぎている場合に更新期間であると判定することを特徴とする。

【００１６】上記更新期間判定部は、上記日付が上記更新予定日と同日である場合に更新期間であると判定することを特徴とする。

【００１７】上記認証書管理装置は、更に、認証局から失効リストを受信する失効リスト受信部を有することを特徴とする。

【００１８】本発明に係る認証書管理装置は、認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする。

（１）更新予定日を含む失効リストを記憶する失効リスト記憶部

（２）日付を管理する日付管理部

（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する更新期間判定部

（４）上記更新期間判定部によって、更新期間であると判定した場合に、更新を催促する情報を出力する更新催促情報出力部。

【００１９】上記更新期間判定部は、上記日付が上記更新予定日を過ぎている場合に更新期間であると判定することを特徴とする。

【００２０】上記更新期間判定部は、上記日付が上記更新予定日と同日である場合に更新期間であると判定することを特徴とする。

【００２１】上記認証書管理装置は、更に、認証局から失効リストを受信する失効リスト受信部を有することを特徴とする。

【００２２】本発明に係る認証書管理方法は、以下の要素を備えることを特徴とする。

（１）有効期限を含む認証書を記憶する工程

（２）日付を管理する工程

（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する工程

（４）更新期間であると判定した場合に、更新を催促する情報を出力する工程。

【００２３】本発明に係る認証書管理方法は、認証局に接続する装置の認証書管理方法であって、以下の要素を

備えることを特徴とする。
（１）有効期限を含む認証書を記憶する工程
（２）日付を管理する工程
（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する工程
（４）更新期間であると判定した場合に、更新要求を認証局に出力する工程。
【００２４】本発明に係る認証書管理方法は、認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする。
（１）更新予定日を含む失効リストを記憶する工程
（２）日付を管理する工程
（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する工程
（４）更新期間であると判定した場合に、更新要求を認証局に出力する工程。
【００２５】本発明に係る認証書管理方法は、認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする。
（１）更新予定日を含む失効リストを記憶する工程
（２）日付を管理する工程
（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する工程
（４）更新期間であると判定した場合に、更新を催促する情報を出力する工程。
【００２６】本発明に係るコンピュータ読み取り可能な記録媒体は、以下の処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする。
（１）有効期限を含む認証書を記憶する処理
（２）日付を管理する処理
（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する処理
（４）更新期間であると判定した場合に、更新を催促する情報を出力する処理。
【００２７】本発明に係るコンピュータ読み取り可能な記録媒体は、以下の処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする。
（１）有効期限を含む認証書を記憶する処理
（２）日付を管理する処理
（３）上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する処理
（４）更新期間であると判定した場合に、更新要求を認証局に出力する処理。
【００２８】本発明に係るコンピュータ読み取り可能な記録媒体は、以下の処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする。
（１）更新予定日を含む失効リストを記憶する処理
（２）日付を管理する処理
（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する処理
（４）更新期間であると判定した場合に、更新要求を認証局に出力する処理。
【００２９】本発明に係るコンピュータ読み取り可能な記録媒体は、以下の処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする。
（１）更新予定日を含む失効リストを記憶する処理
（２）日付を管理する処理
（３）上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する処理
（４）更新期間であると判定した場合に、更新を催促する情報を出力する処理。
【００３０】
【発明の実施の形態】実施の形態１．以下本発明を図面に示す実施例に基づいて説明する。図１は、本発明におけるシステムの構成図である。１３と１４は、データの転送を行なう端末である。端末１３と端末１４は、インターネット１１を介して接続されている。また、認証局１２と端末１３もインターネット１１を介して接続されている。認証局１２と端末１４の間も同様である。
【００３１】図２は、認証書の構成を示す図である。認証書２１には、公開鍵２２と、有効期限２３が含まれている。この例では、端末１３の要求により認証局１２が認証書２１を発行し、端末１３は、認証書２１を受信し、更に端末１４へ転送する。尚、認証書は、ディジタル証明書、ディジタルＩＤ、証明書、認証証などと呼ばれることもある。
【００３２】２２は、公開鍵である。公開鍵２２は、端末１３から端末１４へ送られる暗号データを復号するときに用いられる。
【００３３】２３は、有効期限である。有効期限２３内においてのみ、認証書２１は有効である。従って、端末１３側では、有効期限２３を超える前に更新の手続きをしなければならない。
【００３４】図３は、実施の形態１における端末の構成のうち有効期限の管理に関する部分を示す図である。３１は、アプリケーション部、３２は、表示部、３３は、操作部、３４は、認証書管理部、３５は、更新期間判定部、３６は、更新催促情報出力部、３７は、更新指示入力部、３８は、認証書記憶部、３９は、日付・時刻管理部、４０は、更新要求出力部、４１は、秘密鍵記憶部、４２は、認証書受信部、４３は、認証書識別情報記憶部である。
【００３５】アプリケーション部３１は、データの転送の処理に先立って、認証書の確認を認証書管理部３４へ依頼する。
【００３６】図４は、実施の形態１における認証書管理部による有効期限の管理の処理フローを示す図である。認証書の確認を依頼された認証書管理部３４は、有効期限の管理の処理を開始する。
【００３７】更新期間判定部３５は、認証書記憶部３８

から有効期限を読む（Ｓ１０１）。更新期間判定部３５は、更に日付・時刻管理部３９から日付を読む（Ｓ１０２）。そして、更新する期間に入っているかを判定する（Ｓ１０３）。この例では、有効期限－日付が、予め定められた更新期間に含まれるか否かを判定する。例えば、更新期間が２週間に設定されている場合に、有効期限－日付が１３日となれば、更新する期間に入っていると判断する。

【００３８】更新する期間に入っていなければ、更新要求出力部４０は、アプリケーション部３１に更新不要であった旨を通知し、処理を終了する（Ｓ１０４）。

【００３９】更新する期間に入っていれば、更新期間判定部３５は、更新催促情報出力部３６に認証書の更新が必要である旨を伝える。更新催促情報出力部３６は、表示部３２に認証書の更新を催促する情報を表示させる（Ｓ１０５）。

【００４０】ここで、ユーザー１５は、続けて認証書を更新するか（これを、更新指示という。）、あるいは、認証書の更新をせずに終了するかを選択し、操作部３３を介して入力する。

【００４１】更新指示が入力されなかった場合には、処理を終了する。

【００４２】更新指示が入力された場合には、更新要求出力部４０は、認証局１２へ更新要求を送信する。この例では、更新前の認証書識別情報と、ユーザー識別情報を併せて送信する。これによって、認証局１２は、新しい秘密鍵と公開鍵を作成し、新しい認証書と、新しい認証書識別情報と、新しい秘密鍵を端末１３に送信する。

【００４３】認証書受信部４２は、新しい認証書と、新しい認証書識別情報と、新しい秘密鍵を受信し（Ｓ１０８）、新しい認証書を認証書記憶部３８に、新しい認証書識別情報を認証書識別情報記憶部４３に、新しい秘密鍵を秘密鍵記憶部４１に記憶させる（Ｓ１０９～Ｓ１１１）。

【００４４】続いて、認証書管理部３４は、認証書送付の処理を行なう。図５は、実施の形態１における端末の構成のうち認証書送付に関する部分を示す図である。５１は、認証書送信要否確認情報出力部、５２は、認証書送信指示入力部、５３は、認証書送信部である。

【００４５】図６は、実施の形態１における認証書管理部による認証書送付の処理フローを示す図である。

【００４６】認証書送信要否確認情報出力部５１は、表示部３２に認証書の送信の要否を確認する表示をさせる。ユーザー１５は、この表示により、続けて認証書の送信を行なうか（これを認証書送信指示という。）、あるいは、認証書の送信を行なわずに終了させるかを判断し、操作部３３に入力する。

【００４７】認証書送信指示入力部５２に認証書送信指示が入力されなかった場合には（Ｓ１１２）、終了する。

【００４８】認証書送信指示入力部５２に認証書送信指示が入力された場合には（Ｓ１１２）、認証書記憶部３８から新しい認証書を読み（Ｓ１１３）、それを端末１４に送信する（Ｓ１１４）。

【００４９】認証書管理部３４による認証書確認の処理が終了すると、アプリケーション部３１は、端末１４に対してデータの転送を行なう。このとき、秘密鍵記憶部４１に記憶された秘密鍵を用いてデータの暗号化を行なう。

【００５０】尚、更新要求出力部４０から認証局１２へ送信される更新要求は、認証局１２の方式に依存する。この例では、認証局１２から秘密鍵も受信する方法を示した。この場合の鍵の作成は、認証局１２が行なうので、更新要求は、更新前の認証書識別情報と、ユーザー識別情報で足りる。一方、端末１３で鍵の作成を行なう場合には、認証書管理部３４で予め鍵を作成し、作成した秘密鍵を秘密鍵記憶部４１に記憶し、更新要求には、更新前の認証書識別情報と、ユーザー識別情報の他に、公開鍵も含める。

【００５１】また、この実施例では、Ｓ１０１で、更新期間判定部３５は、認証書記憶部３８から有効期限を読み、Ｓ１０２で、更に日付・時刻管理部３９から日付を読み、Ｓ１０３で、更新する期間に入っているかを判定するように構成されている例を示したが、時刻を判定の条件に加えることも有効である。認証書２１の中の有効期限２３に時刻が含まれ、更新期間が時刻を含めて管理される場合には、更新期間判定部３５は、認証書記憶部３８から時刻を含めた有効期限を読み、日付・時刻管理部３９から現在の日付と時刻を読み、Ｓ１０３で、更新する期間に入っているかを判定する。例えば、更新する期間の長さが４８時間で、有効期限が１０月１０日の午後３時の場合には、１０月８日の午後２時は更新する期間外となり、１０月８日の午後４時は更新する期間内となる。また、認証書２１の中の有効期限２３に時刻が含まれていない場合であっても、特定時刻に更新が可能となるときには、更新期間判定部３５は、日付・時刻管理部３９から日付と時刻を読み、Ｓ１０３で、更新する期間に入っているかを判定する。例えば、認証局による更新処理が午前１０（特定時刻）から開始されると仮定し、更新する期間の長さが１０日で、有効期限が１０月２０日の場合に、１０月１０日の午前９時（特定時刻前）は更新する期間外となり、１０月１０日の午前１１時（特定時刻後）は更新する期間内となる。

【００５２】本実施の形態により、認証書の有効期限を過ぎる前に、ユーザーに認証書の更新を促し、認証書の有効期限切れを未然に防止することができる。

【００５３】また、ユーザーが認証書の更新の要否を選択できるので、より高い安全性確保のために他の認証書更新方法を採用するなど、柔軟な運用が可能である。

【００５４】更に、認証書の送信についても、ユーザー

がその要否を選択できるので、同様に他の認証書送付方法を採用するなど、柔軟な運用が可能である。

【００５５】実施の形態２．本実施の形態では、認証書の更新と、認証書の送信を自動的に処理する形態について説明する。

【００５６】図７は、実施の形態２における端末の構成を示す図である。更新期間判定部３５は、更新指示を直接更新要求出力部４０に伝えるように構成されている。また、認証書受信部４２が認証書を受信し、認証書記憶部３８に認証書が記憶されると、自動的に認証書送信部５３が認証書を送信するように構成されている。

【００５７】図８は、実施の形態２における認証書管理部の処理フローを示す図である。Ｓ１０１からＳ１０３は、実施の形態１と同様である。

【００５８】更新期間判定部３５が更新する期間に入っていると判断した場合には、更新指示を更新要求出力部４０に伝える。更新要求出力部４０はこれを受けて更新要求を出力する（Ｓ１０７）。Ｓ１０７からＳ１１１は、実施の形態１と同様である。

【００５９】認証書送信部５３は、Ｓ１１１の処理に続いて認証書を読み（Ｓ１１３）、端末１４へ送信する（Ｓ１１４）。

【００６０】この例では、認証書の更新と、認証書の送信の両方を自動的に処理する形態について説明したが、一方のみを自動化し、更新催促情報出力部３６と更新指示入力部３７を付加する構成、あるいは、認証書送信要否確認情報出力部５１と認証書送信指示入力部５２を付加する構成とすることも有効である。

【００６１】本実施の形態により、認証書の更新と、認証書の送信を自動的に処理するので、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼動を促進することができる。

【００６２】実施の形態３．本実施の形態では、失効リストの更新を自動化する形態について説明する。

【００６３】図９は、失効リストの構成を示す図である。６１は、失効リスト更新日、６２は、失効リスト更新予定日、６３、６４は、失効した認証書の認証書識別情報である。失効リスト更新日６１は、この失効リストを更新した日付である。失効リスト更新予定日６２は、次に失効リストを更新する予定の日付である。また、失効した認証書の認証書識別情報６３、６４で識別される認証書は、使用できない。

【００６４】図１０は、実施の形態３における端末の構成を示す図である。３１は、アプリケーション部、３４は、認証書管理部、３９は、日付・時刻管理部、７１は、更新期間判定部、７２は、失効リスト記憶部、７３は、更新要求出力部である。

【００６５】図１１は、実施の形態３における認証書管理部の処理フローを示す図である。アプリケーション部３１は、動作の開始時等の適当な時期に、失効リストの確認を認証書管理部３４に依頼する。

【００６６】更新期間判定部７１は、失効リスト記憶部７２から失効リスト更新予定日６２を読む（Ｓ２０１）。また、日付・時刻管理部３９から、日付を読む。そして、両者を比較し、その時点で失効リスト更新予定日６２を過ぎていなければ、更新不要の旨を通知し（Ｓ２０４）、処理を終了する。

【００６７】一方、比較の結果、その時点で失効リスト更新予定日６２を過ぎていれば、更新要求出力部７３に対して更新指示を伝え、更新要求出力部７３は認証局１２へ失効リストの更新要求を出力する。

【００６８】失効リスト受信部７４は、認証局１２から更新された失効リストを受信する（Ｓ２０６）。そして、失効リスト記憶部７２で更新された失効リストを記憶する。

【００６９】また、この実施例では、更新期間判定部７１による比較の結果、その時点で失効リスト更新予定日６２を過ぎていれば、更新要求出力部７３に対して更新指示を伝える構成を示したが、同日の場合も更新指示を伝えるようにすることも有効である。

【００７０】更新期間判定部７１の判定の条件に、時刻を加えることも有効である。例えば、失効リスト更新予定日６２に更新予定時刻が含まれている場合には、更新期間判定部７１は、Ｓ２０１で更新予定日と更新予定時刻を読み、日付・時刻管理部３９から、現在の日付と時刻を読み、時刻を含めて両者を比較し、判定する。また、失効リスト更新予定日６２に更新予定時刻が含まれていない場合であっても、特定時刻に更新が可能となるときには、更新期間判定部７１は、日付・時刻管理部３９から日付と時刻を読み、更新する期間に入っているかを判定する。例えば失効リストの更新予定時刻が午後３時と決まっている場合には、更新予定日と同日であっても、午後２時であれば更新予定時刻前であるので更新する期間外となり、午後４時であれば更新予定時刻後であるので更新期間内となる。

【００７１】これにより、失効リストの更新を自動化し、ユーザーの管理行為の負担を軽減し、併せて失効リストが最新であることを保証し、認証の有効性を担保することができる。

【００７２】実施の形態４．本実施の形態では、失効リストの更新を催促する形態について説明する。

【００７３】図１２は、実施の形態４における端末の構成を示す図である。８１は、更新催促情報出力部、８２は、更新指示入力部である。

【００７４】図１３は、実施の形態４における認証書管理部の処理フローを示す図である。Ｓ２０１からＳ２０３までは、実施の形態３と同様である。

【００７５】更新期間判定部７１による比較の結果、その時点で失効リスト更新予定日６２を過ぎていれば、更新催促情報出力部８１に失効リストの更新が必要である

13

旨を伝える。更新催促情報出力部８１は、表示部３２に失効リストの更新を催促する情報を表示させる（Ｓ３０１）。

【００７６】ここで、ユーザー１５は、続けて失効リストを更新するか（これを、更新指示という。）、あるいは、失効リストの更新をせずに終了するかを選択し、操作部３３を介して入力する（Ｓ３０２）。

【００７７】更新指示が入力されなかった場合には、処理を終了する。

【００７８】更新指示が入力された場合には、更新要求出力部７３は、認証局１２へ更新要求を送信する。これによって、認証局１２は、新しい失効リストを端末１３に送信する。Ｓ２０５以降は、実施の形態３と同様である。

【００７９】ユーザーが失効リストの更新の要否を選択できるので、より高い安全性確保のために他の失効リスト更新方法を採用するなど、柔軟な運用が可能である。

【００８０】

【発明の効果】認証書の有効期限を過ぎる前に、ユーザーに認証書の更新を促し、認証書の有効期限切れを未然に防止することができる。

【００８１】ユーザーが認証書の更新の要否を選択できるので、より高い安全性確保のために他の認証書更新方法を採用するなど、柔軟な運用が可能である。

【００８２】認証書の送信についても、ユーザーがその要否を選択できるので、同様に他の認証書送付方法を採用するなど、柔軟な運用が可能である。

【００８３】認証書の更新と、認証書の送信を自動的に処理するので、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼動を促進することができる。

【００８４】失効リストの更新を自動化し、ユーザーの管理行為の負担を軽減し、併せて失効リストが最新であることを保証し、認証の有効性を担保することができる。

【００８５】ユーザーが失効リストの更新の要否を選択できるので、より高い安全性確保のために他の失効リスト更新方法を採用するなど、柔軟な運用が可能である。

【図面の簡単な説明】

14

【図１】　本発明におけるシステムの構成図である。

【図２】　認証書の構成を示す図である。

【図３】　実施の形態１における端末の構成のうち有効期限の管理に関する部分を示す図である。

【図４】　実施の形態１における認証書管理部による有効期限の管理の処理フローを示す図である。

【図５】　実施の形態１における端末の構成のうち認証書送付に関する部分を示す図である。

【図６】　実施の形態１における認証書管理部による認証書送付の処理フローを示す図である。

【図７】　実施の形態２における端末の構成を示す図である。

【図８】　実施の形態２における認証書管理部の処理フローを示す図である。

【図９】　失効リストの構成を示す図である。

【図１０】　実施の形態３における端末の構成を示す図である。

【図１１】　実施の形態３における認証書管理部の処理フローを示す図である。

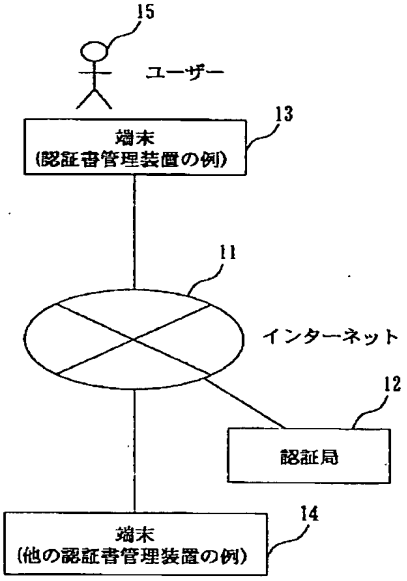
【図１２】　実施の形態４における端末の構成を示す図である。

【図１３】　実施の形態４における認証書管理部の処理フローを示す図である。

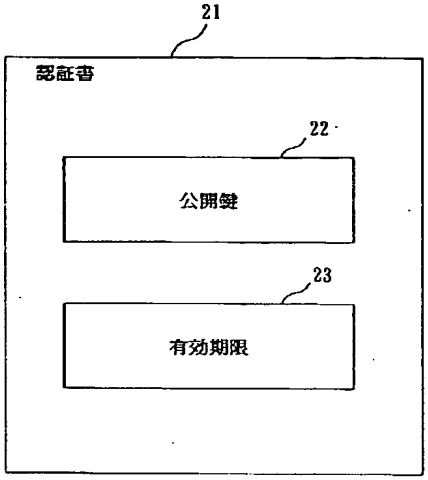
【符号の説明】

１１　インターネット、１２　認証局、１３　端末、１４　端末、１５　ユーザー、２１　認証書、２２　公開鍵、２３　有効期限、３１　アプリケーション部、３２　表示部、３３　操作部、３４　認証書管理部、３５　更新期間判定部、３６　更新催促情報出力部、３７　更新指示入力部、３８　認証書記憶部、３９　日付・時刻管理部、４０　更新要求出力部、４１　秘密鍵記憶部、４２　認証書受信部、４３　認証書識別情報記憶部、５１　認証書送信要否確認情報出力部、５２　認証書送信指示部、５３　認証書送信部、６１　失効リスト更新日、６２　失効リスト更新予定日、６３　失効した認証書の認証書識別情報、６４失効した認証書の認証書識別情報、７１　更新期間判定部、７２　失効リスト記憶部、７３　更新要求出力部、７４　失効リスト受信部、８１　更新催促情報出力部、８２　更新指示入力部。

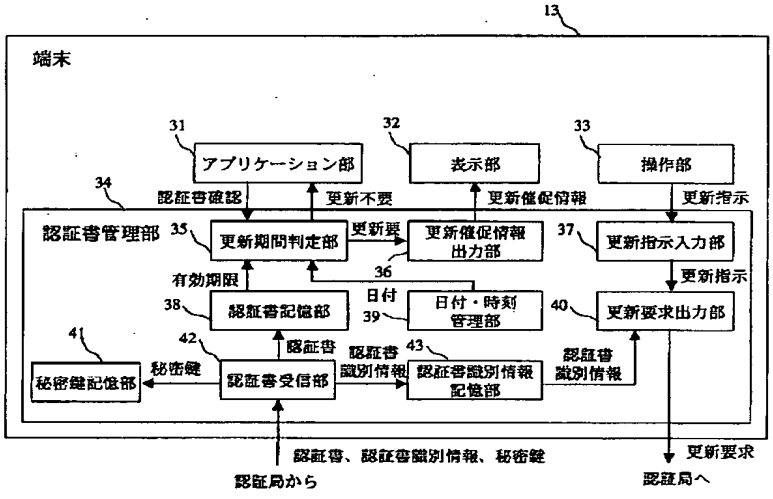
【図１】


15
ユーザー
端末
(認証書管理装置の例)
13
11
インターネット
12
認証局
端末
(他の認証書管理装置の例)
14

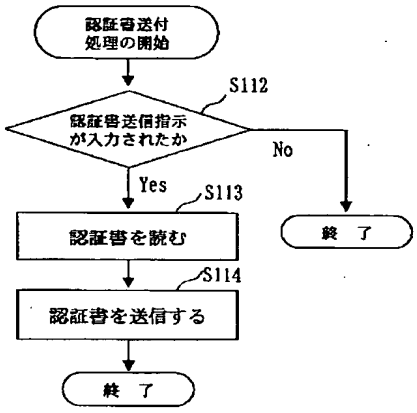
【図２】


21
認証書
22
公開鍵
23
有効期限

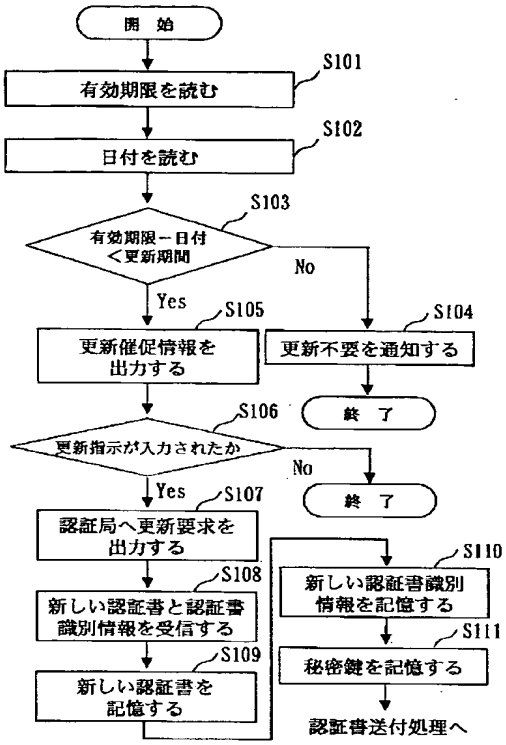
【図３】


13
端末
31
アプリケーション部
32
表示部
33
操作部
34
認証書確認
更新不要
更新催促情報
更新指示
認証書管理部
35
更新期間判定部
更新要
更新催促情報
出力部
37
更新指示入力部
36
有効期限
更新指示
38
認証書記憶部
日付
39
日付・時刻
管理部
40
更新要求出力部
41
42
認証書
認証書
識別情報
43
認証書
識別情報
秘密鍵記憶部
秘密鍵
認証書受信部
認証書識別情報
記憶部
認証書
識別情報
認証書、認証書識別情報、秘密鍵
認証局から
更新要求
認証局へ

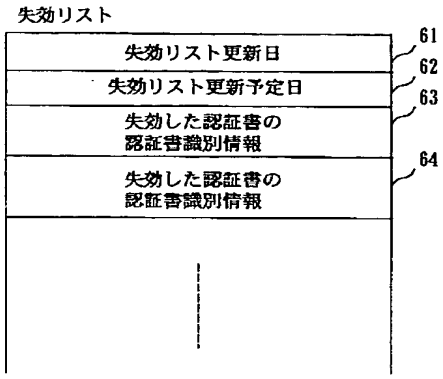
【図６】


認証書送付
処理の開始
S112
認証書送信指示
が入力されたか
No
Yes
終 了
S113
認証書を読む
S114
認証書を送信する
終 了

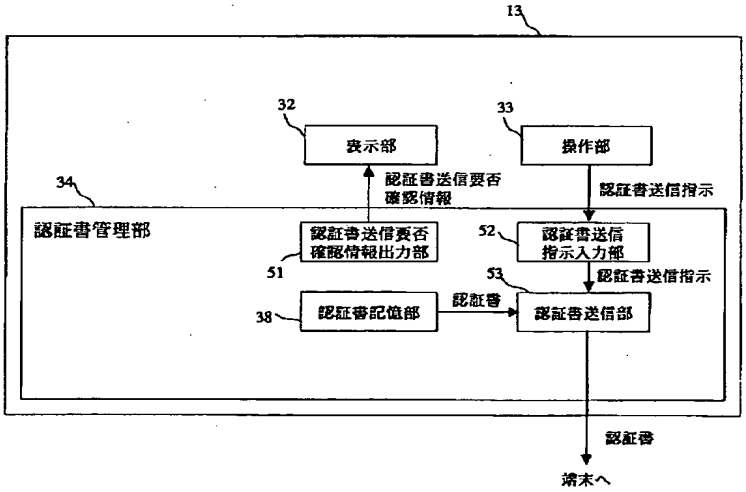
【図４】


開 始
S101
有効期限を読む
S102
日付を読む
S103
有効期限－日付
＜更新期間
No
Yes
S105
更新催促情報を
出力する
S104
更新不要を通知する
終 了
S106
更新指示が入力されたか
No
Yes
終 了
S107
認証局へ更新要求を
出力する
S108
新しい認証書と認証書
識別情報を受信する
S109
新しい認証書を
記憶する
S110
新しい認証書識別
情報を記憶する
S111
秘密鍵を記憶する
認証書送付処理へ

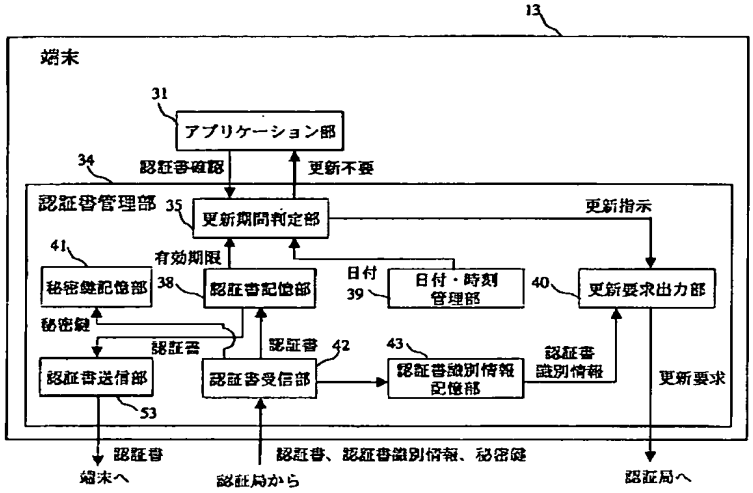
【図９】


失効リスト
失効リスト更新日
61
失効リスト更新予定日
62
失効した認証書の
認証書識別情報
63
失効した認証書の
認証書識別情報
64

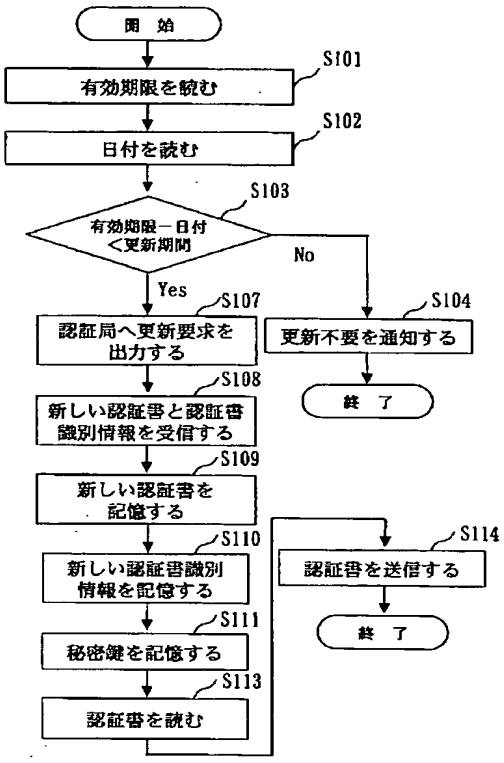
【図５】


13
32
表示部
33
操作部
認証書送信要否
確認情報
認証書送信指示
34
認証書管理部
認証書送信要否
確認情報出力部
51
52
認証書送信
指示入力部
認証書送信指示
53
38
認証書記憶部
認証書
認証書送信部
認証書
端末へ

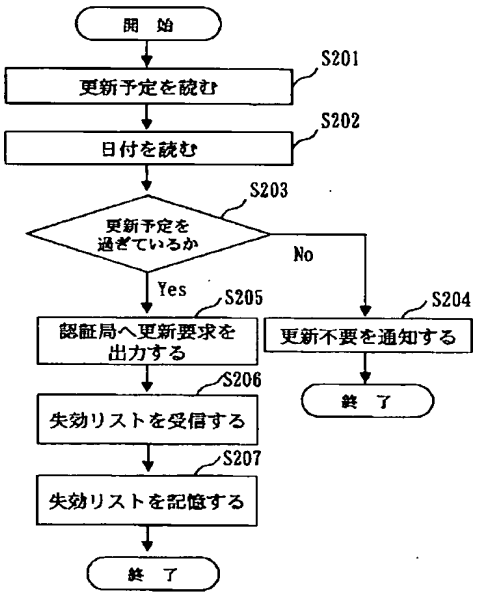
【図７】


13
端末
31
アプリケーション部
34
認証書確認
更新不要
認証書管理部
35
更新期間判定部
更新指示
41
有効期限
秘密鍵記憶部
38
認証書記憶部
日付
39
日付・時刻管理部
40
更新要求出力部
秘密鍵
認証書
認証書
42
43
認証書識別情報
認証書識別情報記憶部
認証書
識別情報
更新要求
認証書送信部
53
認証書
端末へ
認証書、認証書識別情報、秘密鍵
認証局から
認証局へ

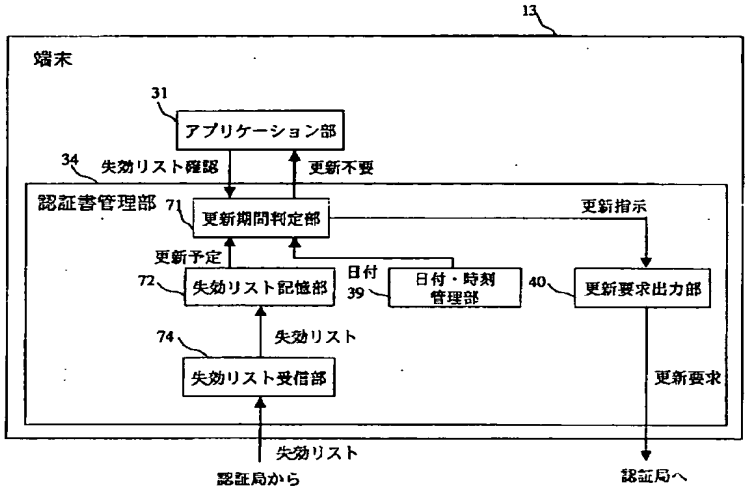
【図８】


開　始
S101
有効期限を読む
S102
日付を読む
S103
有効期限－日付
＜更新期間
No
Yes
S107
認証局へ更新要求を
出力する
S104
更新不要を通知する
終　了
S108
新しい認証書と認証書
識別情報を受信する
S109
新しい認証書を
記憶する
S110
新しい認証書識別
情報を記憶する
S111
秘密鍵を記憶する
S113
認証書を読む
S114
認証書を送信する
終　了

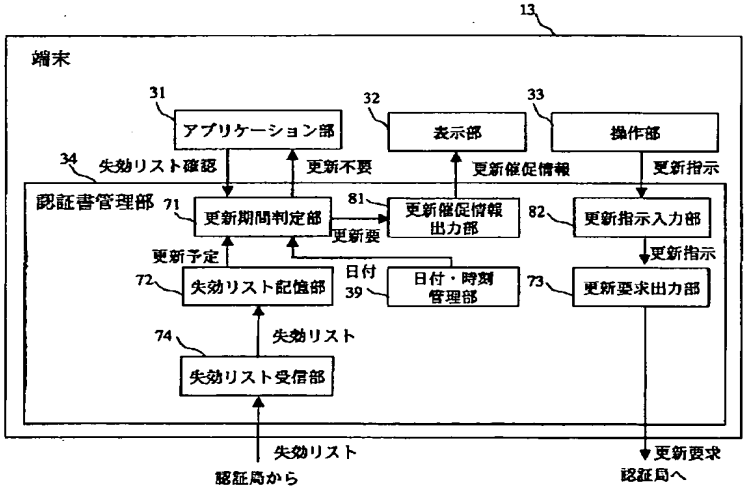
【図１１】


開　始
S201
更新予定を読む
S202
日付を読む
S203
更新予定を
過ぎているか
No
Yes
S205
認証局へ更新要求を
出力する
S204
更新不要を通知する
終　了
S206
失効リストを受信する
S207
失効リストを記憶する
終　了

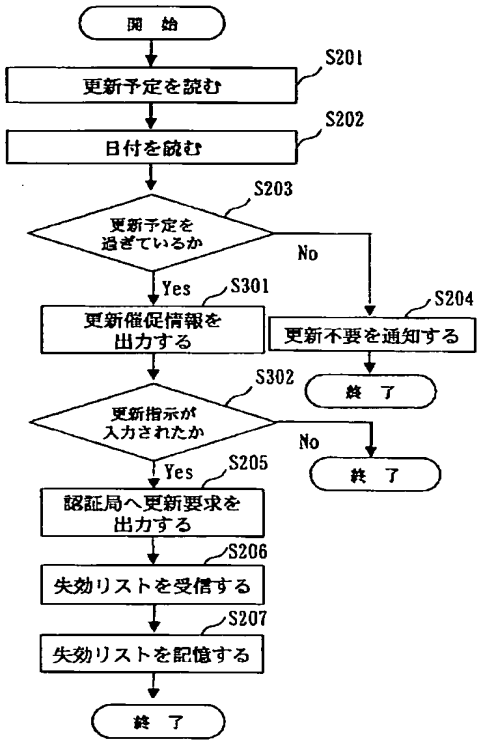
【図１０】


13
端末
31
アプリケーション部
34
失効リスト確認
更新不要
認証書管理部
71
更新期間判定部
更新指示
更新予定
72
失効リスト記憶部
日付
39
日付・時刻管理部
40
更新要求出力部
74
失効リスト
失効リスト受信部
更新要求
失効リスト
認証局から
認証局へ

【図１２】


13
端末
31
アプリケーション部
32
表示部
33
操作部
34
失効リスト確認
更新不要
更新催促情報
更新指示
認証書管理部
71
更新期間判定部
81
更新催促情報出力部
82
更新指示入力部
更新要
更新予定
更新指示
72
失効リスト記憶部
日付
39
日付・時刻管理部
73
更新要求出力部
74
失効リスト
失効リスト受信部
失効リスト
更新要求
認証局から
認証局へ

【図１３】



フロントページの続き

Ｆターム(参考) 5B049 AA01 CC00 CC31 GG02 GG04
5B089 GA21 GB02 HA10 JB22 KA17
KB11
5J104 AA07 AA11 KA01 KA05 MA02
PA07